МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Алтайский государственный педагогический университет»
(ФГБОУ ВО «АлтГПУ»)

УТВЕРЖДАЮ
проректор по образовательной и
международной деятельности

_____С.П. Волохов

Информационная безопасность АИС

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационных технологий**

Учебный план ПМ01.03.04_2022.plx
01.03.04 Прикладная математика

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану	144	Виды контроля в семестрах:
в том числе:		зачеты 7
аудиторные занятия	64	
самостоятельная работа	78	

Программу составил(и):
ктн, Доц., Скурыдина Е.М. _____

Рабочая программа дисциплины
Информационная безопасность АИС

разработана на основании ФГОС ВО - бакалавриат по направлению подготовки 01.03.04 Прикладная математика (приказ Минобрнауки России от 15.01.2018 г. № 11)

составлена на основании учебного плана 01.03.04 Прикладная математика (Уровень: бакалавриат; квалификация: бакалавр), утвержденного Учёным советом ФГБОУ ВО «АлтГПУ» от 25.04.2022, протокол № 9.

Рабочая программа одобрена на заседании кафедры
Информационных технологий

Протокол № 7 от 18.02.2022 г.
Срок действия программы: 2022-2026 уч.г.
Зав. кафедрой Абрамкин Геннадий Петрович

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	11 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	22	22	22	22
Лабораторные	42	42	42	42
Контроль самостоятельной работы	2	2	2	2
Итого ауд.	64	64	64	64
Контактная работа	66	66	66	66
Сам. работа	78	78	78	78
Итого	144	144	144	144

1.1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1.1	формирование у студентов знаний и умений, которые образуют теоретический и практический фундамент в области теоретических основ информационной безопасности, навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах образовательных учреждений.

1.2. ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.2.1	формирование знаний о современных тенденциях угроз информационной безопасности, о нормативных правовых документах по защите информации, а также о современных методах и средствах обеспечения информационной безопасности в экономических информационных системах;
1.2.2	формирование умений выявлять угрозы информационной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности;
1.2.3	формирование навыков владения приемами разработки политики безопасности предприятия и навыками использования методов и средств обеспечения информационной безопасности в информационных системах.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.ДВ.06
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Проектирование информационных систем
2.1.2	Компьютерные сети, интернет и мультимедиа технологии
2.1.3	Программирование
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита информации в БД

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-11.1: Анализирует возможности программирования процедур для выявления попыток несанкционированного доступа к данным
ПК-11.2: Применяет средства программирования для разработки автоматизированных процедур выявления
ПК-10.1: Определяет показатели и критерии эффективности системы безопасности, проводит их расчет и анализ
ПК-10.2: Оценивает уровень и состояние системы безопасности данных на уровне БД
ПК-6.1: Анализирует возможных угроз для безопасности данных
ПК-6.2: Осуществляет выбор основных средств поддержки информационной безопасности на уровне БД
ПК-5.1: Выполняет резервное копирование БД и восстановление БД
ПК-5.2: Управляет доступом к БД
ПК-5.3: Проводит установку и настройку программного обеспечения (ПО) для обеспечения работы пользо-вателей с БД
ПК-4.1: Проводит регистрацию статистических объектов
ПК-4.2: Осуществляет актуализацию данных статистических регистров
ПК-4.3: Формирует выборочные совокупности на основании данных статистических регистров
ПК-3.1: Осуществляет подбор исходных данных для осуществления расчетов
ПК-3.2: Проводит расчет агрегированных и производных статистических показателей
ПК-3.3: Выполняет балансировку и взаимную увязку статистических показателей
УК-2.1: Формулирует цель деятельности и обеспечивающие ее достижение задачи, выбирает оптимальные способы их решения
УК-2.2: Планирует достижение цели с учетом правового поля, имеющихся ресурсов и ограничений в сфере профессиональной деятельности
УК-2.3: Реализует в профессиональной сфере разработанный проект
ПК-3.4: Разрабатывает аналитические материалы
ПК-5.4: Мониторинг работы БД, сбор статистической информации о работе БД

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	методические подходы к подбору исходных данных для осуществления расчетов.
3.1.2	аналитические приемы, процедуры, методические подходы и правила формирования докладов, презентаций, публикаций.
3.1.3	методики осуществления контроля актуальности данных статистического регистра и утвержденные процедуры взаимодействия между государственными органами по актуализации данных статистического регистра.
3.1.4	общие основы решения практических задач по созданию резервных копий, восстановлению БД и проверке корректности восстановленных данных Специальные знания по работе с установленной БД, восстановлению и проверке корректности восстановленных данных
3.1.5	основы управления учетными записями пользователей
3.1.6	полный состав ПО, позволяющего поддерживать работу пользователей с БД, а также регламенты и процедуры установки и настройки ПО, позволяющего поддерживать работу пользователей с БД Специальные знания по работе с установленной БД
3.1.7	угрозы безопасности БД и способы их предотвращения
3.1.8	инструменты обеспечения безопасности БД и их возможности
3.1.9	программно-технические средства защиты данных от несанкционированного доступа, их возможности
3.1.10	способы и методы несанкционированного доступа к данным и механизмы противодействия попыткам несанкционированного доступа.
3.2	**Уметь:**
3.2.1	подбирать исходные данные для осуществления расчетов.
3.2.2	анализировать результаты расчетов и грамотно представлять их в аналитических материалах.
3.2.3	взаимодействовать с другими государственными организациями в целях актуализации данных статистического регистра.
3.2.4	выполнять регламентные процедуры по резервированию и восстановлению данных
3.2.5	применять специальные процедуры управления правами доступа пользователей
3.2.6	применять специальные процедуры установки ПО для поддержки работы пользователей с БД
3.2.7	выявлять угрозы безопасности на уровне БД
3.2.8	разрабатывать мероприятия по обеспечению безопасности на уровне БД.
3.2.9	создавать и настраивать автоматизированные процедуры выявления попыток несанкционированного доступа к данным.
3.2.10	выявлять попытки несанкционированного доступа к данным.
3.3	**Владеть:**
3.3.1	навыками подбора данных для расчетов.
3.3.2	навыками представления аналитических материалов в виде докладов, презентаций, публикаций
3.3.3	навыками контроля актуальности данных статистического регистра
3.3.4	способами выбора действий из известных; контроля, оценки и корректировки действий
3.3.5	специальными знаниями по работе с установленной БД
3.3.6	основами анализа структур базы данных.
3.3.7	процедурами настройки программного обеспечения и контроля результатов для поддержки работы пользователей с БД.
3.3.8	способами разворачивания и настройки программно-аппаратных средств защиты данных.
3.3.9	приемами защиты от несанкционированного доступа к данным, с использованием средств программирования.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Сущность и понятия информационной безопасности				

1.1	Основные аспекты защищенности, как цели информационной безопасности. /Лек/	7	2	УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
1.2	Содержание информационной безопасности исходя из формирования активной защиты критических интересов и пассивной защиты, как создания условий для развития общества и экономики. /Ср/	7	2	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
1.3	Различия в методах обеспечения информационной безопасности по данным направлениям. /Ср/	7	2		Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 2. Законодательный уровень информационной безопасности				
2.1	Российское и зарубежное законодательство в области ИБ /Лек/	7	4	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 3. Угрозы информационной безопасности				

3.1	Классификация угроз. Значимость угроз. Вероятность реализации угроз. /Лек/	7	4	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 4. Каналы утечки и несанкционированного доступа к конфиденциальной информации				
4.1	Классификация. Технические каналы утечки информации. Технические средства промышленного шпионажа. /Лек/	7	4	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 5. Системы защиты информации. Кадровое и ресурсное обеспечение защиты информаци				
5.1	Факторы и условия, определяющие степень эффективности защиты информации /Лек/	7	4	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6

5.2	Значение и состав кадрового обеспечения защиты информации. /Ср/	7	4	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 6. Инженерно-техническая защита информации				
6.1	Общие положения инженерно-технической защиты. /Лек/	7	4	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
6.2	Методы инженерно-технической защиты информации. Методы физической защиты информации. /Ср/	7	4	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 7. Настройка параметров безопасности операционной системы Windows				
7.1	Написание отчета /Ср/	7	5	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6

7.2	Выполнение лабораторной работы: Настройка параметров безопасности операционной системы Windows /Лаб/	7	4	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 8. Локальная политика безопасности в операционной системе Windows				
8.1	Выполнение лабораторной работы: Локальная политика безопасности в операционной системе Windows /Лаб/	7	4	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
8.2	Написание отчета /Ср/	7	5	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 9. Установка и настройка средств защиты информации				
9.1	Выполнение лабораторной работы: Установка и настройка средств защиты информации /Лаб/	7	4	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6

9.2	Написание отчета /Ср/	7	5	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 10. Шифр Цезаря. Шифрование файлов с помощью программы TrueCrypt				
10.1	Выполнение лабораторной работы: Шифр Цезаря. Шифрование файлов с помощью программы TrueCrypt /Лаб/	7	6	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
10.2	Написание отчета /Ср/	7	5	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 11. Организация защиты документов средствами пакета Microsoft Office				

11.1	Выполнение лабораторной работы: Организация защиты документов средствами пакета Microsoft Office /Лаб/	7	6	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
11.2	Написание отчета /Ср/	7	5	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 12. Электронная подпись				
12.1	Выполнение лабораторной работы: Электронная подпись /Лаб/	7	6	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
12.2	Написание отчета /Ср/	7	5	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 13. Настройка параметров безопасности Интернет браузеров				

13.1	Выполнение лабораторной работы: Настройка параметров безопасности Интернет браузеров /Лаб/	7	6	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
13.2	Написание отчета /Ср/	7	6	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 14. Средства защиты компьютера от вирусов				
14.1	Эвристический анализ /Ср/	7	6	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 15. Рекомендации по использованию различных программ в ОУ				
15.1	Технические средства по использованию различных программ в ОУ /Ср/	7	6	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6

	Раздел 16. Меры по созданию безопасной информационной системы в образовательном учреждении				
16.1	Угрозы информационной безопасности /Ср/	7	8	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
	Раздел 17. Средства защиты информации				
17.1	Методы защиты /Ср/	7	10	УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
17.2	Организационные средства защиты информации /Лаб/	7	6	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
17.3	Зачет /Зачёт/	7	0	УК-2.1 УК-2.2 УК-2.3 ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2 ПК-11.1 ПК-11.2 ПК-10.1 ПК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Перечень индикаторов достижения компетенций, форм контроля и оценочных средств

УК-2.1. Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения.
УК-2.2. Умеет анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.
УК-2.3. Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.
ПК 3.1. Знает технологии проектирования ИС.
ПК.3.2. Умеет применять элементы технологий проектирования ИС; осуществлять и обосновывать выбор проектных решений по видам обеспечения информационных систем.
ПК 3.3. Владеет навыками проектирования экономических информационных систем или их частей (модулей).
ПК 4.1. Знает теоретические основы экономики фирмы, методы технико- экономического анализа, структуру технического задания на разработку информационной системы.
ПК.4.2. Умеет проводить расчет экономической эффективности ИС, составлять техническое задание на разработку информационной системы.
ПК 4.3. Владеет навыками исследования эффективности функционирования информационных систем организации, разработки технического задания.
ПК 5.1. Знает методы формального описания бизнес-процессов, методы моделирования прикладных (бизнес) процессов и предметной области.
ПК. 5.2. Умеет составлять описание прикладных процессов, разрабатывать модели прикладных (бизнес) процессов и предметной области.
ПК 5.3. Владеет навыками построения моделей прикладных (бизнес) процессов и предметной области.
ПК 6.1. Знает основы процесса внедрения информационных систем.
ПК. 6.2. Умеет работать в команде проекта по внедрению информационных систем.
ПК 6.3. Владеет навыками участия в работах по внедрению информационных систем.
ПК-11.1. Знает правила создания презентации; методологию, модели, методы и средства прикладных информационных технологий для создания информационных систем в различных предметных областях
ПК-11.2. Умеет находить организационно управленческие решения в нестандартных ситуациях, создавать проекты и управлять проектами в области рекламы и связей с общественностью фирмы, организации; осуществлять презентацию полученных результатов и начальное обучение пользователей; формулировать и осуществлять постановку задач в терминах предметной области пользователя; презентовать информационную систему.
ПК-11.3. Владеет навыками презентации информационной системы; навыками выбора класса ИС для автоматизации в соответствии с требованиями к ИС и ограничениями; способами выбора ИС на основании преимуществ и недостатков существующих способов; навыками расчета совокупной стоимости владения ИС

5.2. Технологическая карта достижения индикаторов

Вопросы для самоконтроля 20 баллов
Задания для лабораторных работ 40 баллов
Тематика докладов, сообщений 20 баллов
Вопросы к зачету 20 баллов

5.3. Формы контроля и оценочные средства

Тестовые задания

1. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
a) меры обеспечения целостности;
b) административные меры;
c) меры обеспечения конфиденциальности.

2. Дублирование сообщений является угрозой:
a) доступности;
b) конфиденциальности;
c) целостности.

3. Вредоносное ПО Melissa подвергает атаке на доступность:
a) системы электронной коммерции;
b) геоинформационные системы;
c) системы электронной почты.

4. Выберите вредоносную программу, которая открыла новый этап в развитии данной области.
a) Melissa.
b) Bubble Boy.
c) ILO VE YOU.

5. Самыми опасными источниками внутренних угроз являются:

a) некомпетентные руководители;
b) обиженные сотрудники;
c) любопытные администраторы.

6. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности.
a) просчеты при администрировании информационных систем;
b) необходимость постоянной модификации информационных систем;
c) сложность современных информационных систем.

7. Агрессивное потребление ресурсов является угрозой:
a) доступности
b) конфиденциальности
c) целостности

Тематика докладов, сообщений:
1. Разработка комплексной системы защиты информации предприятия.
2. Защита облачных сервисов в системах электронного документооборота.
3. Программный комплекс ограничения функциональности условно-бесплатного программного обеспечения, распространяемого в исходных кодах.
4. Правовые основы защиты информации в РФ.
5. Методы и средства удалённого доступа.
6. Автоматизация управления производственным предприятием и анализ его эффективности.
7. Гражданско-правовая защита информации конфиденциального характера.
8. Разработка информационной системы документооборота.
9. Актуальность проблемы информационной безопасности.
10.Понятия и определения в информационной безопасности.
11. Основные составляющие информационной безопасности
12. Анализ способов нарушений информационной безопасности.
13. Использование защищенных компьютерных систем.
14. Основные определения и критерии классификации угроз.
15. Основные закономерности возникновения и классификация угроз информационной безопасности.

Задания для лабораторных работ:
1. Используя основные положения части 4, главы 70 Гражданского кодекса РФ решить следующую ситуационную задачу: Гражданин Алексеев создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием «Alex 3D» и зарегистрировал на него свои права. 20.09.2012 этот гражданин заключил договор с компанией «MoscowTechnology» и передал свои имущественные права на распространение своего программного продукта сроком на один год. После заключения договора компания «MoscowTechnology» распространила версию программы «Alex 3D» с предварительной модификацией данного программного продукта без ведома автора. Имеет ли место в данной ситуации нарушение авторского права гражданина Алексеева? 2. Зашифровать пословицу или поговорку тремя методами: методом Цезаря, методом Гронсфельда и методом Вижинера: «Уменье работать дороже золота»

Вопросы для самоконтроля:
1. Сканеры портов. Обзор. Возможности.
2. Применение сканеров портов.
3. Криптографические протоколы. Применение, характеристики.
4. Причины существования дыр в системе безопасности.
5. Сканеры уязвимостей. Возможности, ограничения.
6. Сетевые анализаторы. Выбор расположения.
7. Практическое применение сетевых анализаторов.
8. Системы обнаружения вторжений. Выбор расположения системы обнаружения.
9. Классификация firewall’ов и определение политики firewall’а.
10. Политика безопасности современных операционных систем.
11. Электронная цифровая подпись

Вопросы к зачету:
1. Информационная безопасность.
2. Основные определения.
3. Содержание и задачи процесса управления информационной безопасностью информационная безопасность в системе национальной безопасности Российской Федерации.
4. Государственная информационная политика.
5. Угрозы информационной безопасности.
6. Классификация и анализ угроз.
7. Вредоносное программное обеспечение.
8. Примеры угроз доступности.

9. Основные угрозы целостности.
10. Основные угрозы конфиденциальности.
11. Оценка уязвимости информации.
12. Система с полным перекрытием.
13. Управление рисками.
14. Основные теории защиты информации.
15. Модели безопасности.
16. Методы формирования функций защиты.
17. Стратегии защиты информации.
18. Методы и системы защиты информации.
19. Криптография.
20. Криптоанализ. Криптографические хеш-функции.
21. Обеспечиваемая шифром степень защиты.
22. Криптоанализ и атаки на криптосистемы.
23. Платформы. Сеть Фейштеля.
24. Дифференциальный и линейный криптоанализ.
25. Используемые критерии при разработке алгоритмов.
26. Криптографические стандарты DES и ГОСТ 28147–89.
27. Алгоритм DES. Шифрование. Дешифрование. Проблемы DES.
28. Контроль целостности.
29. Генераторы электромагнитных импульсов: эффекты, возникающие от внешнего электромагнитного воздействия на АС и СВТ.
30. Методы защиты АС и СВТ от внешнего электромагнитного воздействия»: экранирование, создание преднамеренных помех, кодировка сигнала.
31. Программные средства автоматизации процедур управления информационной безопасности и анализа политики информационной безопасности.
32. Программные средства поддержки процессов управления информационной безопасности.
33. Пути и каналы утечки информации и их обобщенная модель.
34. Классификация каналов утечки информации.
35. Угрозы доступности.
36. Угрозы целостности.
37. Угрозы конфиденциальности.
38. Методы сбора сведений для вторжения в сеть.
39. Обобщенная модель нарушителя безопасности информации.
40. Распределенные атаки на отказ от обслуживания.
41. Вирусы и механизмы их работы.
42. Классификации вирусов. Среда обитания. Способ заражения среды обитания. Деструктивная возможность. Особенности алгоритма вируса.
43. Методы обнаружения и удаления вирусов.
44. Антивирусная стратегия. Антивирусная защита.
45. Основные функции современных антивирусов.
46. Типовая структура корпоративной сети.
47. Способы НСД к каналам передачи данных.
48. Основные пути обеспечения безопасности информации.

5.4. Оценка результатов обучения в соответствии с индикаторами достижения компетенций

Удовл. Пороговый уровень: Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности; принципы, методы и средства решения стандартных задач обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач обеспечения информационной безопасности.

Хорошо. Базовый уровень: Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности; принципы, методы и средства решения стандартных задач обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы с учетом задач обеспечения информационной безопасности. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности; решать стандартные задачи обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологии. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач обеспечения информационной безопасности; навыками составления технической документации на различных этапах жизненного цикла

информационной системы.

Отлично. Высокий уровень: Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности; принципы, методы и средства решения стандартных задач обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы с учетом задач обеспечения информационной безопасности. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач обеспечения информационной безопасности; решать стандартные задачи обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности; применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач обеспечения информационной безопасности; навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности; навыками составления технической документации на различных этапах жизненного цикла информационной системы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Издание	Экз.
Л1.1	В. А. Галатенко	Основы информационной безопасности: учебное пособие — Москва : ИНТУИТ : Ай Пи Ар Медиа, 2020 — URL: http://www.iprbookshop.ru/97562.html	9999
Л1.2	Д. А. Скрипник	Общие вопросы технической защиты информации: учебное пособие — Москва ; Саратов : ИНТУИТ : Ай Пи Ар Медиа, 2020 — URL: http://www.iprbookshop.ru/89451.html	9999
Л1.3	К. Е. Климентьев	Введение в защиту компьютерной информации: учебное пособие — Самара : Изд-во Самарского университета, 2020 — URL: https://e.lanbook.com/book/189043	9999

6.1.2. Дополнительная литература

	Авторы, составители	Издание	Экз.
Л2.1	В. Н. Костин	Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей: учебное пособие — Москва : Издательский Дом МИСиС, 2018 — URL: http://www.iprbookshop.ru/98200.html	9999
Л2.2	О. И. Солонская	Средства защиты информации: учебное пособие — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021 — URL: https://www.iprbookshop.ru/117115.html	9999
Л2.3	В. Н. Костин	Методы и средства защиты компьютерной информации: криптографические методы для защиты информации: учебное пособие — Москва : Издательский Дом МИСиС, 2018 — URL: https://www.iprbookshop.ru/98201.html	9999
Л2.4	А. С. Леонтьев	Защита информации: учебное пособие — Москва : МИРЭА, 2021 — URL: https://e.lanbook.com/book/182491	9999
Л2.5	А. Ю. Ермакова	Криптографические методы защиты информации: учебно-методическое пособие — Москва : МИРЭА, 2021 — URL: https://e.lanbook.com/book/176563	9999
Л2.6	С. М. Авдошин, А. А. Савельева, В. А. Сердюк	Технологии и продукты Microsoft в обеспечении информационной безопасности: учебное пособие — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) : Ай Пи Ар Медиа, 2021 — URL: https://www.iprbookshop.ru/102070.html	9999

6.3.1 Перечень программного обеспечения

6.3.1.1	Пакет LibreOffice
6.3.1.2	Пакет OpenOffice.org
6.3.1.3	Операционная система семейства Windows
6.3.1.4	Операционная система семества Linux
6.3.1.5	Интернет браузер
6.3.1.6	Программа для просмотра электронных документов формата pdf, djvu
6.3.1.7	Медиа проигрыватель
6.3.1.8	Программа 7zip

6.3.2 Перечень информационных справочных систем

6.3.2.1	Президентская библиотека имени Б. Н. Ельцина
6.3.2.2	Сетевая электронная библиотека педагогических вузов // Электронно-библиотечная система Лань / Издательство Лань
6.3.2.3	Национальная электронная библиотека : федеральная государственная информационная система / Министерство культуры Российской Федерации, Российская государственная библиотека
6.3.2.4	Межрегиональная аналитическая роспись статей : поиск статей в российской периодике (МАРС) / АРБИКОН
6.3.2.5	МЭБ. Межвузовская электронная библиотека / Новосибирский государственный педагогический университет
6.3.2.6	Электронная библиотека НПБ / Алтайский государственный педагогический университет, Научно-педагогическая библиотека
6.3.2.7	eLIBRARY.RU : научная электронная библиотека
6.3.2.8	Цифровой образовательный ресурс IPR Smart / Ай Пи Ар Медиа
6.3.2.9	Гарант: информационное-правовое обеспечение

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	1. Оборудованные учебные аудитории, в том числе с использованием видеопроектора и подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Университета.
7.2	2. Аудитории для самостоятельной работы с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Университета.
7.3	3. Аудитория с персональными компьютерами на каждого обучающегося.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Лабораторные работы выполняются студентом в составе 1 человека по каждому индивидуальному проектному заданию. Подготовка к следующей лабораторной работе должна производиться в урочное время. В течение времени, отведенного по расписанию, студенты получают от преподавателя индивидуальное задание, изучают теоретическую часть, соответствующую выполняемой работе, знакомятся с образцовой задачей и на ее основе выполняют индивидуальное задание по принципу подобия и по «нарастанию» нового материла. По итогам лабораторных работ готовится отчет. При защите работы, которая проходит в виде презентации-защиты, студент должен показать достаточные теоретические знания и практические навыки подготовки проектного задания, на основе использования современных информационных и компьютерных технологий. Каждая работа должна получить дифференцированную оценку по 100 бальной системе для представления экзаменатору по данному курсу. Эти оценки позволяют судить о качестве работы студента в семестре и объективно оценивать студента на экзамене. Профессиональная компетенция будущего учителя обеспечивается лекционно-практическим курсом, основанным на коммуникативно-деятельностном системном подходе. Основным результатом освоения дисциплины является понимание магистром реальных учебных ситуаций и осознанное, целенаправленное применение методических знаний в различных педагогических условиях. В систему подготовки будущего магистра входят: - теоретическая подготовка на лекциях; - профессиональная подготовка студентов, реализуемая на лабораторных занятиях, а также при выполнении специальной самостоятельной работы. Реализация программы предусматривает следующие образовательные технологии: В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбор конкретных ситуаций, психологические и иные тренинги) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся. В рамках учебных курсов должны быть предусмотрены встречи с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов. Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 60% аудиторных занятий (определяется требованиями ФГОС с учетом специфики ООП). Занятия лекционного типа для соответствующих групп студентов не могут составлять более 30% аудиторных занятий (определяется соответствующим ФГОС)). Специальная самостоятельная работа студентов, обязательная для выполнения при изучении дисциплины, представлена в разделе «Технологическая карта дисциплины», размещённом в Учебно-методическом комплексе дисциплины (далее УМКД). Методические рекомендации по выполнению конкретного вида самостоятельной работы размещены в УМКД в соответствии со следующей структурой: • алгоритм выполнения; • описание ресурсов, необходимых для решения (тексты, фрагменты документов, образовательных программ и т.д.); • критерии оценивания задания. Конкретные методические рекомендации по подготовке к практическим и лабораторным занятиям, а также по выполнению определенных видов специальной самостоятельной работы представлены в Учебно-методическом комплексе дисциплины на кафедре. Методические рекомендации для студентов, осваивающих дисциплину по индивидуальному учебному плану. Студенты, переведенные на индивидуальный учебный план, до начала занятий по дисциплине должны обратиться к преподавателю и получить пакет заданий по дисциплине для самостоятельного овладения материалом, а также определить с преподавателем точки рубежного контроля и способы дистанционного взаимодействия

Методические рекомендации для обучающихся (с ОВЗ)
Под специальными условиями для получения образования обучающимися с ограниченными возможностями здоровья понимаются условия обучения, воспитания и развития, включающие в себя использование специальных образовательных

программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования. Построение образовательного процесса ориентировано на учет индивидуальных возрастных, психофизических особенностей обучающихся, в частности предполагается возможность разработки индивидуальных учебных планов. Реализация индивидуальных учебных планов сопровождается поддержкой тьютора (родителя, взявшего на себя тьюторские функции в процессе обучения, волонтера). Обучающиеся с ОВЗ, как и все остальные студенты, могут обучаться по индивидуальному учебному плану в установленные сроки с учетом индивидуальных особенностей и специальных образовательных потребностей конкретного обучающегося. При составлении индивидуального графика обучения для лиц с ОВЗ возможны различные варианты проведения занятий: проведение индивидуальных или групповых занятий с целью устранения сложностей в усвоении лекционного материала, подготовке к семинарским занятиям, выполнению заданий по самостоятельной работе. Для лиц с ОВЗ, по их просьбе, могут быть адаптированы как сами задания, так и формы их выполнения. Выполнение под руководством преподавателя индивидуального проектного задания, позволяющего сочетать теоретические знания и практические навыки; применение мультимедийных технологий в процессе ознакомительных лекций и семинарских занятий, что позволяет экономить время, затрачиваемое на изложение необходимого материала и увеличить его объем. Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации преподаватели, в соответствии с потребностями студента, отмеченными в анкете, и рекомендациями специалистов дефектологического профиля, разрабатывает фонды оценочных средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов с ОВЗ устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). Лицам с ОВЗ может быть предоставлено дополнительное время для подготовки к ответу на экзамене, выполнения задания для самостоятельной работы. При необходимости студент с ограниченными возможностями здоровья подает письменное заявление о создании для него специальных условий в Учебно-методическое управление Университета с приложением копий документов, подтверждающих статус инвалида или лица с ОВЗ.